Title (en)
MESSAGE VERIFICATION

Title (de)
NACHRICHTENÜBERPRÜFUNG

Title (fr)
VÉRIFICATION DE MESSAGE

Publication
EP 3357187 A4 20190522 (EN)

Application
EP 15905276 A 20150930

Priority
FI 2015050647 W 20150930

Abstract (en)
[origin: WO2017055676A1] According to an example aspect of the present invention, there is provided an apparatus comprising at least one processing core configured to obtain, from a timestamp, a truncated timestamp comprising a first number of least significant bits of the timestamp and not comprising at least one most significant bit of the timestamp, to derive a hash value based at least in part on the timestamp, a payload and a secret value, and to compile a first message comprising the truncated timestamp, the payload and, at least in part, the hash value, and a transmitter configured to be directed by the at least one processing core, to transmit the first message toward a recipient.

IPC 8 full level
H04L 9/32 (2006.01); **G06F 21/60** (2013.01); **H04L 43/00** (2022.01); **H04L 67/01** (2022.01)

CPC (source: EP US)
G06F 21/64 (2013.01 - EP US); **H04L 9/3239** (2013.01 - EP US); **H04L 9/3297** (2013.01 - EP US); **H04L 9/40** (2022.05 - US); **H04L 43/106** (2013.01 - US); **H04L 63/123** (2013.01 - US); G06F 2221/2151 (2013.01 - EP US); H04L 2209/30 (2013.01 - EP US)

Citation (search report)
- [A] US 2003005284 A1 20030102 - EUCHNER MARTIN [DE]
- [A] US 2013103948 A1 20130425 - BAIG ATTAULLAH [US]
- [A] WOEI-JIUNN TSAUR ET AL: "A Secure Smart-Card-based Password Authenticated Key Agreement Scheme in Multi-server Environments", SOCIAL COMPUTING (SOCIALCOM), 2010 IEEE SECOND INTERNATIONAL CONFERENCE ON, IEEE, PISCATAWAY, NJ, USA, 20 August 2010 (2010-08-20), pages 999 - 1003, XP031767819, ISBN: 978-1-4244-8439-3
- See references of WO 2017055676A1

Designated contracting state (EPC)
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

DOCDB simple family (publication)
WO 2017055676 A1 20170406; CN 108292994 A 20180717; CN 108292994 B 20210608; EP 3357187 A1 20180808; EP 3357187 A4 20190522; EP 3357187 B1 20201021; US 10893056 B2 20210112; US 2018278623 A1 20180927

DOCDB simple family (application)
FI 2015050647 W 20150930; CN 201580084925 A 20150930; EP 15905276 A 20150930; US 201515764006 A 20150930